Annual 47 CFR § 64.2009(e) CPNI Certification Statement

EB Docket 06-36

Annual 64.2009(e) CPNI Certification Statement for **2019** covering the prior calendar year **2018**.

1. Date filed: **February 14, 2019**
2. Name of company(s) covered by this certification: **Noble Systems Communications, LLC**
3. Form 499 Filer ID: **831220**
4. Name of signatory: **John Simpson**
5. Title of signatory: **President**
6. Certification:

I, John Simpson, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 CFR § 64.2001 *et seq*.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company **has not** taken actions (i.e., proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company **has not** received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 CFR § 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed _____ Date: 2/12/2019

President, Noble Systems Communications, LLC

Attachments: Accompanying Statement explaining CPNI procedures

NOBLE SYSTEMS COMMUNICATIONS LLC
POLICY REGARDING
CUSTOMER PROPRIETARY NETWORK INFORMATION ("CPNI")

Noble Systems Communications ("NSC") has established practices and procedures sufficient to ensure compliance with Section 222 of the Communications Act of 1934, as amended, and the Federal Communication Commission's ("FCC") rules pertaining to CNPI, as set forth in 47 C.F.C. §§ 64.2001- 64.2011 of the FCC's rules. It is the policy of NSC to use CPNI in accordance with these statutory and regulatory requirements. The practices and procedures apply to any director, officer, employee, consultant, agent, affiliate, independent contractor, and professional adviser of, to, or contracted by, NSC (collectively "NSC's Employees").

CPNI includes information 1) that related to the quantity, technical configuration, type, destination, location, and amount of sue of a telecommunications service subscriber to by any customer or a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and 2) information contained in the bills pertaining to telephone exchanges service of telephone toll service received by a customer of a carrier. CPNI does not include subscriber list information, which is customer information published in a telephone directory, such as customer name, address, and telephone number.

NSC provides services to contact center providers ("business-to-business"), including non-interconnected and connected VoIP services. It is also the policy of NSC to obtain the customer's consent before disclosing any of the customer's CPNI outside of NSC. NSC does not use CPNI for marketing campaigns and therefore does not maintain records regarding the usage of CPNI in marketing campaigns. NSC does not market, share, or otherwise sell CPNI information to any third party, except as required by law or regulation, or under confidentiality agreement in accordance with FCC rules, or upon customer request. Pursuant to 47 C.F.R. §64.2005 (a)(1), NSC may share the customer's CPNI with its affiliated entities that provide a service offering to the customer.

NSC has implemented a system to obtain approval and informed consent from its customers prior to any usage of CPNI outside of NSC. The system allows for the status of the customer's CPNI to be easily verified.

NSC has implemented a system for supervisory review regarding compliance with the CPNI rules, including the safeguard of such CPNI information by NSC Employees. NSC Employees undergo training regarding policies governing the use of CPNI. There is also an express disciplinary process in place for violation of the company's practices and procedures regarding treatment of CPNI.

NSC may negotiate alternative authentication procedures for services provided to its business customers that have a dedicated account representative and a contract that specifically addresses NSC's protection of CPNI. Notwithstanding this, any on-line access to CPNI by a customer requires entry of a valid user id and password.

NSC follows industry-standard practices to prevent unauthorized access to CPNI by a person other that the subscriber or NSC's Employees. However, NSC cannot guarantee that these practices will prevent every unauthorized attempt to access, use, or disclose personally identifiable information. Therefore, if an unauthorized disclosure were to occur:

- NSC shall provide notification of the breach within seven (7) days to the United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI") via reporting to www.fcc.gov/eb/CPNI/ and www.cpnireporting.gov.
- NSC may wait an additional seven (7) days from its government notice prior to notifying the affected customers of the breach.
- Notwithstanding the provisions above, NSC is not required to wait the additional seven (7) days to notify its customers if NSC determines there is an immediate risk of irreparable harm to the customers.
- NSC shall maintain records of discovered breaches for a period of at least two (2) years.